



International
Civil Aviation
Organization

Organisation
de l'aviation civile
internationale

Organización
de Aviación Civil
Internacional

Международная
организация
гражданской
авиации

منظمة الطيران
المدني الدولي

国际民用
航空组织

When replying please quote:

Ref.: NT-NR7-8.5 — **E.OSG - NACC76424**

21 December 2018

To: States, Territories and International Organizations

Subject: **Workshop on Civil Aviation Cybersecurity
Buenos Aires, Argentina, 19 to 22 February 2019**

Action
Required: **Your confirmation not later than 1 February 2019**

Sir/Madam,


I wish to send you herewith the ICAO/OAS joint invitation for the Workshop on Civil Aviation Cybersecurity, to be held in Buenos Aires, Argentina, from **19 to 22 February 2019**.

The workshop will be conducted in English, with simultaneous interpretation services into Spanish and it has no registration fee. The specific programme and general information will be sent at the appropriate time. OAS/CICTE will provide a fellowship to participating States through the CICTE Point of Contacts in each State (see attachment). In case you wish to delegate a second participant, please consider that travel expenses for the second participant should be covered by your own Administration. Kindly be sure to indicate this in the OAS/CICTE corresponding nomination form being attached.

With the purpose of providing orientation and support to all States regarding the implementation of the Aviation Cybersecurity Strategy, the attached mnemonic paper note containing the proposed regional strategy for this implementation has been developed

You are kindly requested to complete and return both ICAO and OAS/CICTE Nomination Forms for each participant at your earliest convenience and no later than **1 February 2019**

Accept, Sir/Madam, the assurances of my highest consideration.


Firma Digital ICAO/OAS/ICAO
Digital Signature

Melvin Cintron
for
Regional Director
North American, Central American and
Caribbean (NACC) Regional Office

Enclosure: As indicated

N:\NR - AVSEC-FAL\NR 7-8.5 - OAS-CICTE Assistance\1812-OAS-CICTE Cybersecurity\NACC76424-NACC-StatesInvCybersecurityARG.docx / YTR



OAS | More rights
for more people



SMS-CICTE-820/18
December 6, 2018

Antigua and Barbuda
Argentina
The Bahamas
Barbados
Belize
Bolivia
Brazil
Canada
Chile
Colombia
Costa Rica
Cuba
Dominica
Dominican Republic
Ecuador
El Salvador
Grenada
Guatemala
Guyana
Haiti
Honduras
Jamaica
Mexico
Nicaragua
Panama
Paraguay
Peru
Saint Kitts and Nevis
Saint Lucia
Saint Vincent and the Grenadines
Suriname
Trinidad and Tobago
United States of America
Uruguay
Venezuela

On behalf of the Secretariat of the Inter-American Committee against Terrorism (CICTE) of the General Secretariat of the Organization of American States (GS/OAS), and of the International Civil Aviation Organization, I am pleased to address you for the purpose of inviting your Government to nominate one (1) participant to attend the "Workshop on Civil Aviation Cybersecurity", which will take place in the City of Buenos Aires, Argentina between February 19 and 22, 2019 under the auspices of the Airport Security Police (PSA) of Argentina. If your government wishes to nominate more participants, you can do so, provided that all expenses must be borne by each Member State.

The purpose of this workshop is to create basic awareness about the risks of cybersecurity to the civil aviation authorities of the States, providers of air navigation services, operators of airports and airlines, support institutions of information technology (IT) to aviation, and other partners in the aviation industry. The workshop includes the identification of cyber threats and risks, causes of cyber-attacks, as well as ways of managing and mitigating cyber-attacks. At the conclusion of this workshop, participants are expected to be prepared to conduct a risk assessment and prepare a management plan for the risks of cyber-attacks. This workshop has been designed to assist States to achieve the changes proposed by standard 4.9 of ICAO Annex 17, which requires States to identify information and communication technology systems that may be harmed by cyber-attacks, develop and implement measures to protect these systems against unlawful interference.

The four-day workshop will be conducted in English (although the materials will be available in Spanish), with simultaneous interpretation services. It is aimed at aviation security personnel who are responsible for protecting systems, assets, and information and aviation security equipment. It is desirable that the officials to be trained have the necessary knowledge in aviation security, or basic knowledge of information technology (IT). The nominees with higher and middle management level within the State authorities with risk assessment functions and who also have experience in AVSEC operational matters will have the first priority for this training activity.

Any additional nomination will be wait listed until the nominations of all the States have been received to verify the available spaces. We would appreciate receiving the full attached nomination form through the National Contact Points no later than February 1, 2019.



OAS | More rights
for more people



- Antigua and Barbuda
- Argentina
- The Bahamas
- Barbados
- Belize
- Bolivia
- Brazil
- Canada
- Chile
- Colombia
- Costa Rica
- Cuba
- Dominica
- Dominican Republic
- Ecuador
- El Salvador
- Grenada
- Guatemala
- Guyana
- Haiti
- Honduras
- Jamaica
- Mexico
- Nicaragua
- Panama
- Paraguay
- Peru
- Saint Kitts and Nevis
- Saint Lucia
- Saint Vincent and the Grenadines
- Suriname
- Trinidad and Tobago
- United States of America
- Uruguay
- Venezuela

In this occasion the expenses related to the participation of the nominees will be the responsibility of each participant, or of his government. Additionally, please note that each participant will be responsible for fulfilling the visa and travel requirements to enter Argentina.

If you have any questions or doubts about this invitation, please do not hesitate to contact Ms. Mariana Cardona, Cybersecurity Program Officer (E-mail mcardona@oas.org), Mr. Ricardo Delgado (E-mail rdelgado@icao.int), Mr. José María Peral (E-mail: jmperal@icao.int) or cybersecurity@oas.org.

Please accept the assurances of my highest consideration and esteem.

Cordially,

Alison August Treppel
Executive Secretary
Inter-American Committee
against Terrorism
Organization of American States

Melvin Cintron
Regional Director
ICAO North American Central
America and Caribbean Office

- cc
- OAS Permanent Missions
 - Points of Contact AVSEC**
 - Peter Abraham, Antigua and Barbuda
 - Anthony Kirchner, Aruba
 - Andrew Bonaby, Bahamas
 - Tracey L. Forde-Bailey, Barbados
 - Gilberto Torres, Belize
 - Chris Free, Canada
 - Karen Plourde, Canada
 - Stephen Worth, Canada
 - Ben Hudgin, Canada
 - Shane Bothwell, Cayman Islands
 - Victor Krips, Curacao
 - Earl Charles, Grenada
 - Bouchard Theramene, Haiti
 - Althea Bartley, Jamaica
 - Joseph Irish, Montserrat



OAS | More rights
for more people



Antigua and Barbuda
Argentina
The Bahamas
Barbados
Belize
Bolivia
Brazil
Canada
Chile
Colombia
Costa Rica
Cuba
Dominica
Dominican Republic
Ecuador
El Salvador
Grenada
Guatemala
Guyana
Haiti
Honduras
Jamaica
Mexico
Nicaragua
Panama
Paraguay
Peru
Saint Kitts and Nevis
Saint Lucia
Saint Vincent and the Grenadines
Suriname
Trinidad and Tobago
United States of America
Uruguay
Venezuela

Jos Wilbrink, Netherlands
Royston Griffin, Saint Kitts and Nevis
Eustace Cherry, Saint Lucia
David Robin, Saint Vincent and the Grenadines
Raymond Jacobs, Sint Maarten
Ted Martin, Trinidad and Tobago
OT Aviation Security, United Kingdom
Dan Micklewaite, United Kingdom
Rachel Manis, United States
Lourdes Fernandez, United States
Donald McPhail, ECCAA



ICAO SOUTH AMERICAN REGIONAL OFFICE

MNEMONIC NOTE PAPER

REGIONAL STRATEGY

Workshop on Civil Aviation Cybersecurity Buenos Aires, Argentina, 19 to 22 February 2019	
Regional strategy for aviation security	<p>Aviation security regional strategy for the SAM Region is based in SAM Plan and in the Global Aviation Security Plan (GASeP), where the competent aviation security national authorities in the SAM Region should ensure that actions and tasks of the Roadmap should be implemented by all States, according to the following priority results, clue for the sustainable development of the aviation security systems of the region and to improve the regional connectivity:</p> <ul style="list-style-type: none"> ➤ Increase risk awareness and the response to risks. Understand that risk is essential for policies and measures to be effective, consistent and sustainable. Carrying out risk assessments will help identify deficiencies and vulnerabilities, which can then be addressed urgently in the most practical way possible and with the best use of resources. ➤ Develop a culture of security and human capacity. The promotion of an effective security culture is essential to achieve good results in terms of aviation security. A strong culture of security must be developed from the highest levels of management and within each organization. For aviation security to be effective, it is essential to have well trained, motivated and professional staff. ➤ Improve technological resources and encourage innovation. To promote and apply better technological solutions and innovative techniques can provide the tools to increase the efficiency of aviation security and, at the same time, guarantee operational efficiency. ➤ Improve surveillance and quality assurance. To have effective monitoring and quality control processes at the global, national and local levels is essential to ensure the maintenance and effectiveness of aviation security. ➤ Increase regional cooperation and support. To increase collaboration between the NAM / CAR and SAM ICAO regional offices and among the States, regional organizations and stakeholders will allow achieving key aviation security objectives more quickly and efficiently.
Objectives of the workshop	<p>Taking into account that the current environment of threats and risks requires that aviation security continue to be one of the highest priorities for States and the international community. This was highlighted in Resolution 2309 (2016) of the United Nations Security Council - Threats to international peace and security caused by terrorist acts: aviation security, adopted in September 2016 (UNSC 2309), in which ICAO, States and stakeholders are urged to comply with their obligations</p>

	<p>under the treaties and their international responsibilities in relation to aviation security, and Resolution A39-18 of the ICAO Assembly (Consolidated statement of ICAO standing criteria related to aviation security), in accordance with international law.</p> <p>In Annex 17 Amendment 16, Chapter 4, in Section 4.9 Measures related to cyber-threats, Standard 4.9.1 indicates that States will ensure that information technology systems are identified, and communications and critical data used for the purposes of civil aviation. Also, based on a risk assessment, that States elaborate and implement the corresponding measures to protect themselves from unlawful interference. Also in the Recommended Practice 4.9.2 of the same Section, it tells us that States should ensure that the applied measures in application should protect confidentiality, integrity and availability of the systems and / or critical data identified, in accordance with the risk assessment carried out by the corresponding national authorities. According to the above, the workshop to be held in Buenos Aires, under the auspices of ICAO and the OAS, aims to increase awareness in cyber-threats, have a better understanding of the attack methods used, apply risk analysis techniques to face cyber-threats, and to understand the role and functions of the national Emergency Response Teams (CERT), and the development of useful tools for better coordination and resilience in case of a cyber-attack.</p>
<p>Activities held by the SAM Region related to Cybersecurity</p>	<p>With the signature by ICAO of the Civil Aviation Cybersecurity Action Plan (December 2014) together with other international organizations (i.e., ACI, CANSO, IATA) and Resolution 39-19 of 39 ° Session of the ICAO Assembly on cybersecurity, the AVSEC / FAL Regional Group has created a working group on cybersecurity, which developed a Workshop on Cybersecurity, with the aim of increasing awareness within the aviation industry with regarding cybersecurity, and of providing States with a framework on how to manage cyber-risks faced by the aviation industry.</p>
<p>Current situation of the Sam Region</p>	<p>The SAM Region, together with the SEC-ISD Section of ICAO Montreal, and based on a training needs evaluation to improve and implement the course objectives, considered necessary to develop a bilingual training package (English / Spanish) to:</p> <ul style="list-style-type: none"> ➤ Review the existing documentation developed by CANSO, AIAA, European Union, OAS and other agencies; ➤ Consult with cybersecurity experts in the Region and in other United Nations Agencies; and ➤ Identify and use CMDN Course Designers:
<p>Workshop nature</p>	<p>The workshop includes the identification of cyber threats and risks, identification of cyber-attacks causes, and ways of managing and mitigating cyber-attacks. Participants are expected to be prepared to conduct a risk assessment and to prepare a contingency plan for facing cyber-attacks risks.</p>
<p>Competences to be generated by this workshop</p>	<p>It is expected that participants will gain skills to increase awareness of cyber threats in their States, have a better understanding of the attack methods used, apply risk analysis techniques to deal with cyber threats, and understand the role and functions of the National Computer Emergency Response Teams (CERT), and be able to develop contingency plans in their States in case of cyber-attacks.</p>

Participants' profile	The workshop is addressed to: <ul style="list-style-type: none">➤ Aviation security personnel responsible for protecting aviation security systems, assets, information and equipment;➤ ANS, ATM and CNS personnel who have the necessary knowledge in aviation security, or basic knowledge of technological information (IT); and➤ High and middle management level personnel within the State authorities having risk assessment functions and experience in AVSEC operational matters.
Next steps for the development of the strategy	In compliance with the AVSEC regional strategy and with the GASEP: <ul style="list-style-type: none">➤ Update the material when new requirements are presented and new threats appear;➤ Continue to monitor the implementation of GASEP in the Region; and➤ Link the workshop activities with others related to the updating and incorporation of these threats in the security programmes of the States of the Region and their subsequent implementation.
Contact person in the SAM Office	Mr. Pablo Lampariello AVSEC/FAL Regional Officer ICAO South American Regional Office plampariello@icao.int